Certification Report

TOMITA Tatsuo, Chairman
Information-technology Promotion Agency, Japan
2-28-8 Honkomagome, Bunkyo-ku, Tokyo

IT Product (TOE)

Reception Date of Application (Reception Number)	2022-04-25 (ITC-2811)
Certification Identification	JISEC-C0775
Product Name	TOSHIBA e-STUDIO2525AC/3025AC/3525AC all of the above with FAX Unit and FIPS Hard Disk Kit
Version and Release Numbers	SYS V2.1
Product Manufacturer	TOSHIBA TEC CORPORATION
Conformance of Functionality	PP conformant functionality, CC Part 2 Extended
Protection Profile Conformance	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Certification Identification: JISEC-C0553)
Name of IT Security Evaluation Facility	Information Technology Security Center, Evaluation Department

This is to report that the evaluation result for the above TOE has been certified as follows.
2023-02-22

YANO Tatsuro, Technical Manager
IT Security Technology Evaluation Department
IT Security Center

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following standards prescribed in the "IT Security Evaluation and Certification Scheme Document."

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 5
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 5

Evaluation Result: Pass

"TOSHIBA e-STUDIO2525AC/3025AC/3525AC all of the above with FAX Unit and FIPS Hard Disk Kit, Version SYS V2.1" has been evaluated based on the standards required, in accordance with the provisions of the "Requirements for IT Security Certification" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1 Executive Summary

This Certification Report describes the content of the certification result in relation to IT Security Evaluation of "TOSHIBA e-STUDIO2525AC/3025AC/3525AC all of the above with FAX Unit and FIPS Hard Disk Kit, Version SYS V2.1" (hereinafter referred to as the "TOE") developed by TOSHIBA TEC CORPORATION, and the evaluation of the TOE was completed on 2023-01-31 by Information Technology Security Center, Evaluation Department (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, TOSHIBA TEC CORPORATION, and provide security information to procurement entities and consumers who are interested in the TOE.

Readers of the Certification Report are advised to read the Security Target (hereinafter referred to as the "ST") described in Chapter 10. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOE are described in the ST.

This Certification Report assumes procurement entities who purchase the TOE to be readers. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee an individual IT product itself.

1.1 Product Overview

An overview of the TOE functions and operational conditions is described as follows. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 Protection Profile or Assurance Package

The TOE conforms to the following Protection Profile [14][15] (hereinafter referred to as the "Conformance PP").

> Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015
> (Certification Identification: JISEC-C0553)

1.1.2 TOE and Security Functionality

The TOE is a multifunction product (hereinafter referred to as "MFP"), which has functions such as copy, print, scan and fax.

The TOE provides security functions required by the Conformance PP to prevent the document data processed by the MFP and the setting data etc. affecting security from unauthorized disclosure and alteration.

For these security functions, the validity of the design policy and the accuracy of the implementation were evaluated within the scope of the assurance requirements of the Conformance PP.

Threats and assumptions assumed for the TOE are described in the following sections.

1.1.2.1 Threats and Security Objectives

The following threats are assumed for the TOE.

There are threats that user document data and data affecting security functions, which are assets to be protected by the TOE, may be disclosed or altered by unauthorized operation of the TOE or unauthorized access to the network to which the TOE is connected.

There are also threats that security functions of the TOE may be compromised by the failure of the TOE itself or installation of unauthorized software.

The TOE provides security functions required by the Conformance PP such as identification and authentication, access control, encryption, and digital signature to counter these threats.

1.1.2.2 Configuration and Assumptions

The TOE is assumed to be operated under the following configuration and assumptions.

It is assumed that the TOE is operated in the environment where unauthorized physical access is restricted and it is connected to a LAN separated from the Internet.

The setting, administration and maintenance of the TOE must be performed in accordance with the guidance documents by a trusted administrator. Users of the TOE must have been trained in order to use the TOE securely.

1.1.3 Disclaimers

The following operation is not ensured by this evaluation:

- An environment different from that described in "4.2 Environmental Assumptions"
- TOE with settings different from those described in "7.5 Evaluated Configuration"

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility conducted IT security evaluation and completed in 2023-

01, based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme Document"[1], "Requirements for IT Security Certification"[2], and "Requirements for Approval of IT Security Evaluation Facility"[3] provided by the Certification Body.

1.3 Certification

The Certification Body verified the Evaluation Technical Report [13] and the Observation Reports prepared by the Evaluation Facility as well as evaluation documentation, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure. The certification oversight reviews were also prepared for those concerns found in the certification process. The Certification Body confirmed that all the concerns were fully resolved, and that the TOE evaluation had been appropriately conducted in accordance with the CC ([4][5][6] or [7][8][9]) and the CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report and fully concluded certification activities.

2 Identification

The TOE is identified as follows:

TOE Name:	TOSHIBA e-STUDIO2525AC/3025AC/3525AC all of the above with FAX Unit and FIPS Hard Disk Kit
TOE Version:	SYS V2.1
Developer:	TOSHIBA TEC CORPORATION

The TOE is one of the following:

・Sales area: North America, Europe

TOSHIBA e-STUDIO2525AC with FAX Unit and FIPS Hard Disk kit SYS V2.1
TOSHIBA e-STUDIO3025AC with FAX Unit and FIPS Hard Disk kit SYS V2.1
TOSHIBA e-STUDIO3525AC with FAX Unit and FIPS Hard Disk kit SYS V2.1

Users can verify that a product is the TOE, which is evaluated and certified, by the following means.

Users confirm the following information displayed on the main unit of the MFP, the control panel of the MFP and the print output of the function list as described in the guidance document.

- Model number: One of the following:
  “e-STUDIO2525AC”
  “e-STUDIO3025AC”
  “e-STUDIO3525AC”

- FAX unit:
  For North America: “GD-1370NA-N”
  For Europe: “GD-1370EU”

- FIPS Hard Disk kit GE-1260:
  “9401 TOSHIBA MQ01ABU032BW”

- Software:
  “SYS V2.1”

3 Security Policy

The TOE provides the basic functions of the MFP such as copy, print, scan, and fax functions. It has the functionality to store the user document data in the TOE and to communicate with user terminals and various servers via a network.

The TOE provides security functions that satisfy the requirements of the Conformance PP, to protect the document data processed by the MFP and setting data etc. affecting security.

As the background of the security functions provided by the TOE, user roles, assets, threats, and organizational security policies assumed for the TOE are described in following Section 3.1 to 3.4. Details of the security functions of the TOE are described in Chapter 5.

3.1 Users

The user roles assumed for the TOE are shown in Table 3-1.

Table 3-1 User Roles

Designation	Definition
Normal User	A User who has been identified and authenticated and does not have an administrative role
Administrator	A User who has been identified and authenticated and has an administrative role

3.2 Assets

The assets assumed to be protected by the TOE are shown in Table 3-2, Table 3-3 and Table 3-4. There are two categories of the assets, User Data and TSF Data, as shown in Table 3-2. Furthermore, User Data is classified as shown in Table 3-3 and TSF Data is as shown in Table 3-4.

Table 3-2 Assets

Designation	Category	Definition
D.USER	User Data	Data created by and for Users that do not affect the operation of the TSF
D.TSF	TSF Data	Data created by and for the TOE that might affect the operation of the TSF

Table 3-3 Assets (User Data)

Designation	Type	Definition
D.USER.DOC	User Document Data	Information contained in a User's Document, in electronic or hardcopy form
D.USER.JOB	User Job Data	Information related to a User's Document or Document Processing Job

Table 3-4 Assets (TSF Data)

Designation	Type	Definition
D.TSF.PROT	Protected TSF Data	TSF Data for which alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE, but for which disclosure is acceptable
D.TSF.CONF	Confidential TSF Data	TSF Data for which either disclosure or alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE

3.3 Threats

The threats assumed for the TOE are shown in Table 3-5.

Table 3-5 Threats

Designation	Definition
T.UNAUTHORIZED_ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.
T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.
T.UNAUTHORIZED_UPDATE	An attacker may cause the installation of unauthorized software on the TOE.
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.

3.4 Organizational Security Policies

The organizational security policies required for the TOE are shown in Table 3-6.

Table 3-6 Organizational Security Policies

Designation	Definition
P.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions.
P.AUDIT	Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN.
P.STORAGE_ENCRYPTION	If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.
P.KEY_MATERIAL	Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.
P.FAX_FLOW	If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.

4 Assumptions and Clarification of Scope

This chapter describes the assumptions and the operational environment to operate the TOE as useful information for the assumed readers to determine whether to use the TOE.

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE. The effective performances of the TOE security functions are not assured unless these assumptions are satisfied.

Table 4-1 Assumptions

Designation	Definition
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.
A.NETWORK	The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.
A.TRUSTED_ADMIN	TOE Administrators are trusted to administer the TOE according to site security policies.
A.TRAINED_USERS	Authorized Users are trained to use the TOE according to site security policies.

4.2 Environmental Assumptions

Figure 4-1 shows the operational environment assumed for the TOE. The TOE is installed in a general office and used in an environment connected to the public telephone line and a LAN which is the internal network of the organization. Users operate the control panel of the TOE or a client PC connected to LAN to use the TOE.

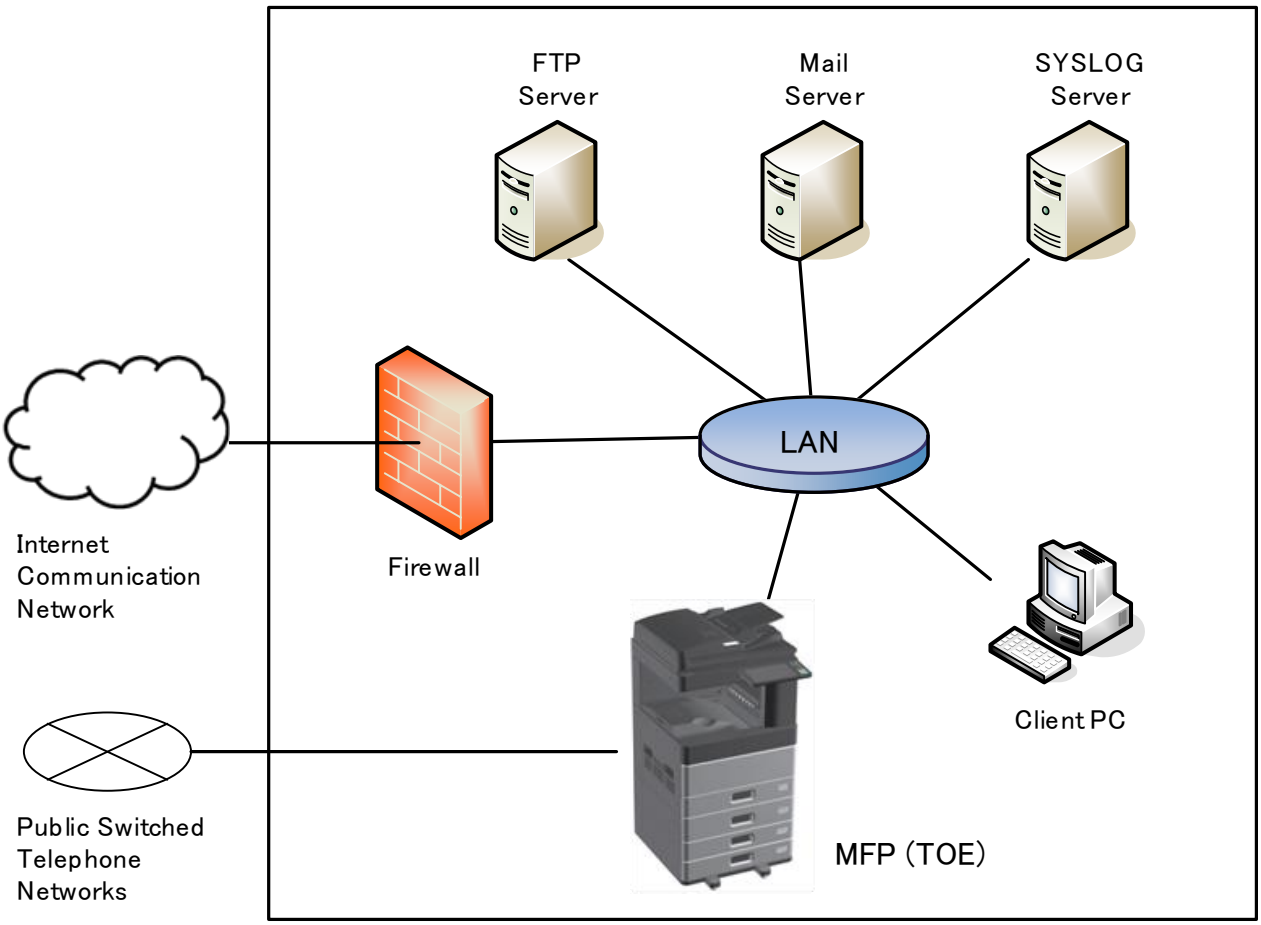

Figure 4-1 Operational Environment of the TOE

The operational environment of the TOE consists of the following components.

(1) Client PC

It is a general PC used by users. The following software is required.

- Printer Driver:
  TOSHIBA Universal Printer Driver2 (Version : 7.222.5412.30)
- Web browser:
  Microsoft Edge

(2) SYSLOG Server (Audit server)

It is an audit server to store the audit log generated by the TOE. It must use the syslog protocol and support TLS 1.2. Installation of this server is mandatory. Syslog-ng 3.14 was used in this evaluation.

(3) Mail Server

The mail server is required when the user document data scanned by the "scan function" is sent as an attachment of an email. It must support TLS 1.2. Sendmail 8.15.2 was used in this evaluation.

(4) FTP Server

The FTP server is required when the user document data scanned by the "scan function" is sent to the specified FTP server. It must support TLS 1.2. ProFTPD 1.3.6 was used in this evaluation.

It should be noted that the reliability of the hardware and the software other than the TOE shown in this configuration is outside the scope of this evaluation. Those are assumed to be trustworthy.

4.3 Clarification of Scope

Secure operation is required so that the communication protocol operates correctly in the client PC and various servers in order to protect the data on the communication path between the TOE and client PC, and the TOE and various servers.

Administrators are responsible for operating servers and client PCs cooperating with the TOE securely.

5 Architectural Information

This chapter explains the scope and the main components of the TOE.

5.1 TOE Boundary and Components

Figure 5-1 shows the composition of the TOE. The TOE is the area surrounded by the frame indicated as TOE in Figure 5-1.

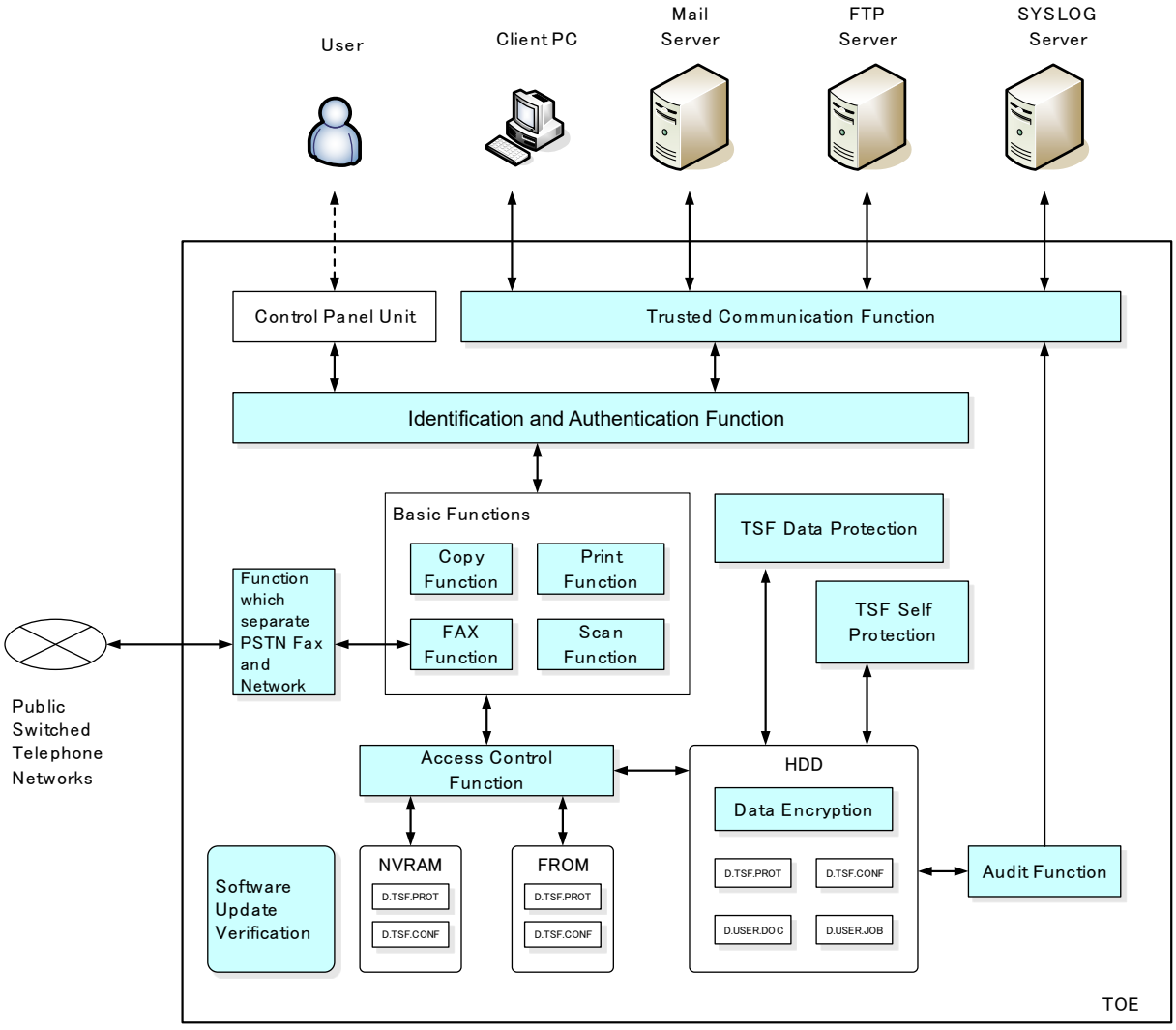

Figure 5-1 TOE boundary

In Figure 5-1, the colored squares within the frame indicated as TOE show the functions provided by the TOE. These functions consist of basic functions and security functions.

The security functions of the TOE are described below. For details on the basic functions, see Chapter 11.

(1) Identification and Authentication Function

This function is a function to identify and authenticate users with the user ID and password when users use the TOE from the control panel of the MFP or the Web browser of a client PC. When using the TOE from the printer driver of a client PC, users are identified by the user ID.

This function has the following functionality to reinforce the identification and authentication.

- Restriction on the minimum password length.
- Account lockout after successive authentication failures.
- Termination of the session if there is no operation for a certain time after the successful authentication.

(2) Access Control Function

This function is a function to control the access to the user data when users operate the basic functions of the MFP on them.

The access control is performed based on the owner information of the user data and on the user's identification information and role.

(3) Data Encryption

This function is a function to store the user document data, etc. in the self-encrypting drive in the TOE.

The self-encryption drive has been validated by JCMVP.

(4) Trusted Communication Function

This function is a function to protect communication data between the TOE and IT devices using encryption communication protocol, TLS 1.2.

(5) TSF Data Protection

This function is a function to control the access to the TSF data in order to restrict the setting, etc. of security functions to administrators.

(6) TSF Self Protection

This function is a function to verify the digital signature of the firmware, etc. at start-up of the TOE.

(7) Software Update Verification

This function is a function to verify the digital signature of new firmware when the firmware is updated.

(8) Audit Function

This function is a function to generate audit logs on audit events relevant to the security functions and send them to an audit server.

(9) Function which separate PSTN Fax and Network

This function is a function to separate the Public Switched Telephone Network (PSTN) and the LAN. The use of the PSTN is limited to fax and no other communication is possible.

5.2 IT Environment

The TOE communicates with servers and client PCs via LAN.

The function of the TOE described in "(4) Trusted Communication Function" works in cooperation with those IT devices and uses the following protocols:

- Client PC (Web browser): HTTP over TLS
- Client PC (Printer driver): IPP over TLS
- SYSLOG server: syslog over TLS
- Mail server: SMTP over TLS
- FTP server: FTP over TLS

6 Documentation

The identification of the guidance documents of the TOE is listed in Table 6-1. TOE users are required to fully understand and comply with the following documents in order to satisfy the assumptions.

Table 6-1 Guidance

Name	Identification
Preparation of Paper	OME21000400
Troubleshooting	OME21000600
Quick Start Guide	OME21001200
Safety Information	OME21001400
Information About Equipment	OME21001600
Copy	OME21001800
Scan	OME21002000
Fax	OME21002200
Template	OME21002600
User Functions	OME21002800
Frequently Asked Questions	OME21003000
Installation	OME21003200
Print	OME21003400
TopAccess	OME21003600
Specifications	OME21003800
High Security Mode	OME210040B0
FAX Unit Precautions for GD-1370	OME21004600
Information to our customers	OMM210083B0

7 Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Facility

Information Technology Security Center, Evaluation Department that conducted the evaluation as the Evaluation Facility is approved under JISEC and is accredited by NITE (National Institute of Technology and Evaluation), the Accreditation Body, which joins Mutual Recognition Arrangement of ILAC (International Laboratory Accreditation Cooperation). It is periodically confirmed that the above Evaluation Facility meets the requirements on the appropriateness of the management and evaluators for maintaining the quality of evaluation.

7.2 Evaluation Approach

The evaluation was conducted in accordance with the assurance requirements in the CC Part 3 required by the Conformance PP using the evaluation methods prescribed in the CEM and the assurance activities of the Conformance PP.

Details for evaluation activities were reported in the Evaluation Technical Report. The Evaluation Technical Report explains the summary of the TOE as well as the content of the evaluation and the verdict for each work unit in the CEM and assurance activity of the Conformance PP.

7.3 Overview of Evaluation Activity

The history of the evaluation conducted is described in the Evaluation Technical Report as follows.

The evaluation started in 2022-04 and concluded upon completion of the Evaluation Technical Report dated 2023-01. The Evaluation Facility received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidence in relation to a series of evaluation conducted. Furthermore, the evaluator conducted the evaluator testing at the developer site in 2022-06.

Concerns found in evaluation activities were issued as the Observation Reports and reported to the developer. Those concerns were reviewed by the developer, and all the concerns were solved eventually.

Concerns in the evaluation process that the Certification Body found were described as the certification oversight reviews and sent to the Evaluation Facility.

After the Evaluation Facility and the developer examined the concerns, those were reflected in the Evaluation Technical Report.

7.4 IT Product Testing

As the verification results of the evidence presented in the evaluation process, the evaluator performed the evaluator independent testing to ensure that the security functions of the product are accurately implemented and the evaluator penetration testing based on the vulnerability assessment.

7.4.1 Developer Testing

The developer testing is not included in the assurance requirements of this evaluation.

7.4.2 Evaluator Independent Testing

The evaluator conducted evaluator independent testing (hereinafter referred to as "independent testing") based on the evidence presented during the evaluation to ensure that the security functions of the product are accurately implemented. The independent testing performed by the evaluator is explained as follows.

1) Independent Testing Environment

The environment for the independent testing is based on the operational environment of the TOE shown in Figure 4-1. The components used in the independent testing environment are listed in Table 7-1.

Table 7-1 Components of Independent Testing

Components	Description
TOE	For North America TOSHIBA e-STUDIO2525AC with FAX Unit and FIPS Hard Disk kit Version: SYS V2.1 For Europe TOSHIBA e-STUDIO3525AC with FAX Unit and FIPS Hard Disk kit Version: SYS V2.1
SYSLOG server	Syslog-ng 3.14
Mail server	Sendmail 8.15.2
FTP server	ProFTPD 1.3.6
Client PC	Web browser : - Microsoft Edge 98.0.1108.50 Printer Driver: - TOSHIBA Universal Printer Driver2 7.222.5412.30

There are following differences between the configuration of the independent testing and the TOE configuration identified in the ST. The evaluator determined that there are no problems with those differences and that the security functions of the TOE configuration identified in the ST can be considered properly tested.

(1) Tested models

In the models of the TOE described in Chapter 2 "TOE identification," there are multiple models due to the following differences:

- Differences in FAX Unit by sales area (Europe, North America)
- Difference in printing speed

The evaluator determined that the security functions of all the models of the TOE can be considered to have been tested by testing the representative two models considering the above differences, because the security functions of each models are the same.

(2) Using additional testing tools

In the independent testing, some testing tools were used to confirm and alter the communication data and to confirm the encryption functions. The validity of those testing tools was confirmed by the evaluator.

2) Summary of the Independent Testing

A summary of the independent testing is as follows.

a. Viewpoints of the Independent Testing

The viewpoints of the independent testing devised by the evaluator based on the requirements of the Conformance PP and on the evaluation documentation submitted for evaluation are shown below.

<Viewpoints of the Independent Testing>

1. Confirm security functions for each Security Functional Requirement (SFR).
2. Confirm that the implementation of the cryptographic algorithms is correct.

b. Independent Testing Outline

An outline of the independent testing that the evaluator performed is as follows.

<Independent Testing Approach>

The behavior of the TOE for inputs using the control panel of the TOE, the client PC and the testing tools was confirmed by following means:

- If the behavior can be confirmed from the external interfaces of the TOE, the external interfaces of the TOE including audit logs are used.
- If the behavior cannot be confirmed from the external interfaces of the TOE, the developer interface of the TOE is used.

<Content of the Performed Independent Testing>

The independent testing was performed on 18 items by the evaluator.

Table 7-2 shows contents of the independent testing corresponding to the viewpoints.

Table 7-2 Content of the Performed Independent Testing

Viewpoint	Outline of the Independent Testing
1	Confirmation of security functions Confirm that all security functions work as the specification with the test items created based on the assurance activities of the Conformance PP for each SFR or the requirements of the SFR.
2	Confirmation of implementation of cryptographic algorithms Confirm the following cryptographic algorithms are implemented as the specification using the test program installed in the TOE. - RSA (key generation, signature generation/verification) - AES-CBC-128, AES-CBC-256 - SHA-1, SHA-256, SHA-384, SHA-512 - HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512 - Hash_DRBG, CTR_DRBG - KDF in Counter Mode

c. Result

All the independent testing performed by the evaluator was correctly completed, and the evaluator confirmed the behavior of the TOE. The evaluator confirmed consistencies between the expected behavior and all the testing results.

7.4.3 Evaluator Penetration Testing

The evaluator devised and performed the evaluator penetration testing (hereinafter referred to as the "penetration testing") on the potentially exploitable vulnerabilities of concern under the assumed environment of use and attack level from the evidence presented in the process of the evaluation. The penetration testing performed by the evaluator is explained as follows.

(1) Summary of the Penetration Testing

A summary of the penetration testing performed by the evaluator is as follows.

a. Vulnerability of Concern

The evaluator searched into the provided documentation and the publicly available

information for the potential vulnerabilities, and then identified the following vulnerabilities which require the penetration testing.

1. There is a concern that unintended network ports of the TOE may be open, and known vulnerabilities may exist in the network services running on the TOE.
2. There is a concern that known vulnerabilities may exist in the Web interface of the TOE.
3. There is a concern that known vulnerabilities may exist in the print processing of the TOE.
4. There is a concern that the identification and authentication function may be bypassed by the malicious input from the control panel of the TOE or Web interface.

b. Penetration Testing Outline

The evaluator performed the following penetration testing to identify potentially exploitable vulnerabilities.

<Penetration Testing Environment>

The penetration testing was performed in the same environment as that of the evaluator independent testing, except for the additional tools for penetration testing. Table 7-3 shows the tools used in the penetration testing.

Table 7-3 Penetration Testing Tools

Name	Outline and Purpose of Use
Nmap 7.9.2	A tool to detect available network service ports.
Nessus 10.2.0	A tool to detect known vulnerabilities at network ports.
OWASP ZAP 2.11.1	A tool to detect known vulnerabilities at Web application.
PRET 0.40	A tool to inspect various vulnerabilities in a printing processing.

<Content of the Performed Penetration Testing>

Table 7-4 shows contents of the penetration testing corresponding to the vulnerabilities of concern.

Table 7-4 Content of the Performed Penetration Testing

Vulnerability	Penetration Testing Outline
1	- Confirm that unexpected network ports of the TOE are not open using Nmap. - Confirm that there are no known vulnerabilities in the available network ports of the TOE using Nessus.
2	- Confirm that there are no known vulnerabilities in the Web interface of the TOE using OWASP ZAP.
3	- Confirm that there are no known vulnerabilities in print processing of the TOE using PRET and exploit codes obtained on the Internet.
4	- Confirm that unexpected behaviour is not observed even if the character strings that may cause unauthrised processing are input in

	the control panel and Web interface of the TOE.

c. Result

In the penetration testing performed by the evaluator, the evaluator did not find any exploitable vulnerabilities that attackers who have the assumed attack potential could exploit.

7.5 Evaluated Configuration

The conditions of the TOE configuration, that are prerequisites for this evaluation, are as described in the guidance documents listed in Chapter 6. In order to use the TOE securely as ensured by the evaluation, the TOE must be set as described in the guidance documents. Different settings are not subject to assurance by this evaluation.

7.6 Evaluation Results

The evaluator had concluded that the TOE satisfies all work units prescribed in the CEM and all assurance activities in the Conformance PP as per the Evaluation Technical Report.

In the evaluation, the following were confirmed.

- PP Conformance:
  Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015

  Protection Profile for Hardcopy Devices - v1.0 Errata #1, June 2017

  Guideline for Certification Application with HCD-PP Conformance [16]
  Temporary treatment regarding FDP_DSK_EXT.1
  Treatment regarding FCS_RBG_ EXT.1 Test
- Security functional requirements: Common Criteria Part 2 Extended
- Security assurance requirements: Common Criteria Part 3 Conformant

As a result of the evaluation, the verdict "PASS" was confirmed for the following assurance components required by the Conformance PP.

ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1

The result of the evaluation is only applied to those which are composed by the TOE corresponding to the identification described in the Chapter 2.

7.7 Evaluator Comments/Recommendations

There is no evaluator recommendation to be addressed to procurement entities.

8 Certification

Based on the evidence submitted by the Evaluation Facility during the evaluation process, the Certification Body has performed certification by checking that the following requirements are satisfied:

1. Contents pointed out in the Observation Reports shall be adequate.
2. Contents pointed out in the Observation Reports shall properly be solved.
3. The submitted documentation was sampled, the content was examined, and the related work units in the CEM and assurance activities of the Conformance PP shall be evaluated as presented in the Evaluation Technical Report.
4. Rationale of the evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.
5. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM and the assurance activities of the Conformance PP.

Concerns found in the certification process were prepared as the certification oversight reviews, and they were sent to the Evaluation Facility. The Certification Body confirmed such concerns pointed out in the certification oversight reviews were solved in the ST and the Evaluation Technical Report and issued this Certification Report.

8.1 Certification Result

As a result of verification of the Evaluation Technical Report, Observation Reports and related evaluation documentation submitted by the Evaluation Facility, the Certification Body determined that the TOE evaluation satisfies the assurance requirements required by the Conformance PP.

8.2 Recommendations

Procurement entities who are interested in the TOE are advised to refer "4.2 Environmental Assumptions" and "7.5 Evaluated Configuration" to make sure the scope of the evaluation and the operational requirements of the TOE meet the operational conditions assumed by each user.

The old audit data will be lost in the case the audit data is not sent and the capacity of the storage area inside the TOE becomes full. Thus the operator has to periodically confirm whether the audit data is sent to the SYSLOG server.

9 Annexes

There is no annex.

10 Security Target

The Security Target [12] of the TOE is provided as a separate document from this Certification Report.

Title:	TOSHIBA e-STUDIO2525AC/3025AC/3525AC all of the above with FAX Unit and FIPS Hard Disk kit Security Target
Version:	2.08
Publication Date:	2023-01-27
Author:	TOSHIBA TEC CORPORATION

11 Glossary

The abbreviations relating to the CC used in this report are listed below.

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

The abbreviations relating to the TOE used in this report are listed below.

MFP	Multifunction Product
PSTN	Public Switched Telephone Network

The abbreviations relating to information technology used in this report are listed below.

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CTR_DRBG	Counter (CTR) mode block cipher algorithm DRBG
DRBG	Deterministic Random Bit Generator
FTP	File Transfer Protocol
HMAC	Keyed-Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
IPP	Internet Printing Protocol
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
TLS	Transport Layer Security

The definitions of terms used in this report are listed below.

Field Replaceable (Unit)	The smallest subassembly that can be swapped in the field to repair a fault.
Hardcopy Device	A system producing or utilizing a physical embodiment of an electronic document or image. These systems include printers, scanners, fax machines, digital copiers, MFPs (multifunction products), MFDs (multifunction devices), “all-

	in-ones" and other similar products.
JCMVP	It is an abbreviation of Japan Cryptographic Module Validation Program.
Copy Function	It is a function to copy and print the user document data scanned from paper documents by user's operation from the control panel.
Scan Function	It is a function to scan paper documents and send the scanned user document data to the mail server and FTP server by user's operation from the control panel.
FAX Function	It is a function to send and receive the document data to and from external fax machines conforming to the G3 standard connected by the PSTN. It consists of the fax transmission function, in which paper documents are scanned and the scanned document data are sent to the external fax machine, and the fax reception function, in which document data sent from an external fax machine are received and printed by user's operation.
Print Function	It is a function to receive the user document data via the LAN from the printer driver of the client PC and print it by user's operation from the control panel.
Assurance Activity	Evaluation work to be performed by an evaluator in order to conform to a PP. It is a supplement of the CEM. In the case of the Conformance PP [14], it is described in the Conformance PP.

12 Bibliography

[1] IT Security Evaluation and Certification Scheme Document, October 2020, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, October 2020, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, October 2021, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 5, April 2017, CCMB-2017-04-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 5, April 2017, CCMB-2017-04-001, (Japanese Version 1.0, July 2017)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-002, (Japanese Version 1.0, July 2017)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-003, (Japanese Version 1.0, July 2017)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 5, April 2017, CCMB-2017-04-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 5, April 2017, CCMB-2017-04-004, (Japanese Version 1.0, July 2017)

[12] TOSHIBA e-STUDIO2525AC/3025AC/3525AC all of the above with FAX Unit and FIPS Hard Disk Kit Security Target, Version 2.08, January 27, 2023, TOSHIBA TEC CORPORATION

[13] TOSHIBA e-STUDIO2525AC/3025AC/3525AC all of the above with FAX Unit and FIPS Hard Disk Kit Evaluation Technical Report, Version 1.4, January 31, 2023, Information Technology Security Center, Evaluation Department

[14] Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Certification

Identification: JISEC-C0553)

[15] Protection Profile for Hardcopy Devices - v1.0 Errata #1, June 2017

[16] Guideline for Certification Application with HCD-PP Conformance, Version 1.8, November 11, 2020, Information-technology Promotion Agency, Japan, JISEC-CERT-2020-A18